UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/999,766	07/23/1997	SCOTT A. MOSKOWITZ	2377/23	4344

29693 7590 10/01/2003

WILEY, REIN & FIELDING, LLP
ATTN: PATENT ADMINISTRATION
1776 K. STREET N.W.
WASHINGTON, DC 20006

EXAMINER	
MEISLAHN, DOUGLAS J	
ART UNIT	PAPER NUMBER
2132	33

DATE MAILED: 10/01/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 33

Application Number: 08/999,766
Filing Date: July 23, 1997
Appellants: MOSKOWITZ ET AL.

Floyd B. Chapman
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10 July 2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 34 and 40-43 with 46-48 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

A substantially correct copy of appealed claim 31 appears on page 1 of Appendix A to the appellant's brief. The minor errors are as follows: the claim as filed says that “the carrier signal is composed of” instead of the appendix's “the carrier signal includes”.

A substantially correct copy of appealed claim 37 appears on pages 2 and 3 of Appendix A to the appellant's brief. The minor errors are as follows: the claim as filed says “into a range” instead of the appendix's “in the range”.

A substantially correct copy of appealed claim 38 appears on page 3 of Appendix A to the appellant's brief. The minor errors are as follows: the claim as filed says “spectral” instead of “spectra” in the second line and “into a range of spectral values” instead of “into a range of sample values” in the third line.

A substantially correct copy of appealed claim 40 appears on page 3 of Appendix A to the appellant's brief. The minor error is as follows: “stet” in line 2 is a misspelling of “set”.

A substantially correct copy of appealed claim 43 appears on pages 3 and 4 of Appendix A to the appellant's brief. The minor errors are as follows: the claim as filed says “a sample window” instead of “the sample windows” in the second line and “window” instead of “windows” as the last word.

A substantially correct copy of appealed claim 44 appears on page 4 of Appendix A to the appellant's brief. The minor errors are as follows: the claim as filed says “window” instead of “windows” in the second line.

Applicant had been required to provide a substitute specification in the first office action. Applicant supplied an exact copy of the originally filed specification, complete with a massive number of typographical errors. The examiner refused entry of the mistake-riddled specification and asked applicant to provide a corrected copy of the specification, a request with which applicant has yet to comply.

(9) Prior Art of Record

5930377	Powell et al.	07-1999
5912972	Barton	06-1999
5530751	Morris	06-1996
EP0581317	Powell et al.	02-1994

Schneier, B. Applied Cryptography, First ed., 1994, pp. 67-68, 224-226.

Bender, W., D. Gruhl, N. Morimoto "Techniques for data hiding", Proc. SPIE vol. 2420: Storage and Retrieval for Image and Video Databases III, pp. 164-173, publ. March 1995.

Cox, I. J. et al. "Secure Spread Spectrum Watermarkings for Multimedia, NEC Research Institute, Technical Report 95-10, 33 pp.

As steganography is both a relatively obscure word and at the focal point of the instant proceedings, a definition is appropriate. Menezes et al. (*Handbook of Applied Cryptography*) define steganography as “that branch of information privacy which attempts to obscure the existence of data through such devices as invisible inks, secret compartments, the use of subliminal channels, and the like.” (page 46, lines 1-3).

Schneier (Applied Cryptography, 2nd ed.) discusses steganography at a bit more length on pages 9 and 10.

> **Steganography** serves to hide secret messages in other messages, such that the secret's very existence is concealed. Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. Historical tricks include invisible inks, tiny pin punctures on selected characters, minute differences between handwritten characters, pencil marks on typewritten characters, grilles which cover most of the message except a few characters, and so on.
>
> More recently, people are hiding secret messages in graphic images. Replace the least significant bit of each byte of the image with the bits of the message. The graphical image won't change appreciably – most graphics standards specify more gradations of color than the human eye can notice – and the message can be stripped out at the receiving end. You can store a 64-kilobyte message in a 1024 x 1024 grey-scale picture this way. Several public-domain programs do this sort of thing.
>
> Peter Wayner's **mimic functions** obfuscate messages. These functions modify a message so that its statistical profile resembles that of something else: the classifieds section of *The New York Times*, a play by Shakespeare, or a newsgroup on the Internet [1584, 1585]. This type of steganography won't fool a person, but it might fool some big computers scanning the Internet for interesting messages.

(10) Grounds of Rejection

Many interpretations can be applied to the term "stega-cipher". The office has chosen to examine three of these; the material in parentheses is possible claim language for the second clause of claim 25 that incorporates the varied interpretations: 1) the swaths of specification chosen as support for "stega-cipher" are extensive enough to be non-limiting, effectively making the term's limitations entirely contained within its immediate meaning ("using steganographic and cipher methods to steganographically encode independent information including a digital watermark into the carrier signal");

2) the specification provides guidelines for the interpretations of "stega-cipher" - the office has interpreted the guidelines for this second scenario to limit the term "stega-cipher" to the selection of an appropriate site for data insertion and the use of a key in the steganographic insertion of material into data ("selecting a portion of the carrier signal that will minimize any perceptible impact of inserting independent information and using a key to steganographically encode independent information including a digital watermark into the carrier signal");

3) the definition of stega-cipher, as given by applicant in the interview on 04 December 2001, is fully read into the claims ("using an algorithm or combination of algorithms to steganographically determine where in the carrier signal data can be hidden 'in plain view' and to use potential data location information, a random or pseudo random seed, and independent information to generate a key that randomly maps the independent information, including a digital watermark, into the carrier signal").

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 25-63 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There is no teaching of using the independent information to form the key. The examiner has interpreted the definition to mean that a key made of a random or pseudo random seed and potential data location information is used to randomly map message data into a carrier signal. The independent information is not used to generate the key. This rejection is

applicable only if the third interpretation of “stega-cipher”, or a new interpretation that likewise requires that the key be derived from the independent information, is used.

2. Claims 25, 27-29, 31-33, 35, 62, and 63 are rejected under 35 U.S.C. 102(a) as being anticipated by Bender et al. (“Techniques for data hiding”).

In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be “invisible” or “inaudible”. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2, Bender is mentioned as encrypting the embedded data. A reading of the section cited as support for the amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but it is not quite entirely clear.

As the above applies to the first interpretation of “stega-cipher”, the original file referred to the second paragraph of section 3.4.1 is a carrier. The independent information is shown in the “binary string (‘code’)” portion of figure 2 on page 172. As described in relation to the original file, the coded independent information is attenuated prior to insertion into the original file. Thus, the addition is done steganographically. In the first line of page 165, Bender et al. talk about digital watermarks being embedded, thereby anticipating its use as independent information. Scrambling with the random wave is a cipher method.

In the second interpretation of "stega-cipher", a key must be used in the process and an insertion area selected. In the first paragraph of section 3.4.1, Bender et al. say that a key, which is pseudo-random noise, is used to modify the independent information, thereby anticipating the use of a key in the steganographic, or data hiding, process. Multiplying by the carrier signal selects where the watermark will be placed.

The third interpretation of "stega-cipher" requires that positions in the original data be selected as optimal for reducing the noticeable impact of information insertion and that the key make use of these locations and a random or pseudo-random seed. As described in the second paragraph of section 3.4.1, the independent information is best spread across the entirety of the available frequency band; in other words, the entirety of the available frequency band is selected as the insertion point. As described in section 3.4, data hiding is optimized by using "as much of the frequency spectrum as possible." This is implemented by the multiplication of the independent information by the carrier signal and the random sequence (section 3.4.1). As such, the steganographic function is the selection of the carrier wave. Furthermore, these two signals read, respectively, on applicant's potential data location information and random or pseudo random seed. Their combined use as modifiers of the independent information accents that they can be viewed, together, as applicant's key. The combination of seed, location information, and independent information is added to Bender et al.'s original file, which reads on mapping the independent information to the original file, or carrier signal as applicant calls it.

As shown by the addition of an attenuated spread data sequence to an original file, the original file includes a continuous analog waveform. Thus claim 27 is anticipated. Claim 28 is anticipated by Bender et al.'s abstract, which lists copyright protecting, a form of rights ownership identification, as a reason for data hiding. Also, at the top of page 165, Bender et al. say that watermarks can mark the ownership of a host signal. With respect to claim 29, Bender et al. say that the key is also needed to decode independent information from a signal encoded with independent information. Claims 31 and 32 are rejected for largely the same reasons as claims 27 and 28. Claim 33 is met by the original embedding of the watermark. That is, the first derivative encoded signal is the original placement of the encoded independent information within the carrier signal. Despite being clause c), the claim does not dictate that the limitations therein occur after those of clauses a) and b). With respect to claim 35, watermarks that convey rights information are anticipated to be difficult to remove from their carrier; their removal would degrade the carrier, making it less legible (see the last sentence of the first paragraph of the introduction). This less legible carrier reads on applicant's second derivative encoded signal. Claims 62 and 63 are met in the third paragraph of the introduction on page 164, which says that degradations of the host (or carrier) signal should be "invisible" or "inaudible".

3. Claims 25-33, 35-39, 62, and 63 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Powell et al. (EPO 0 581 317 A2, in the Response to Arguments section, this reference is referred to as EP-Powell).

Powell et al. show a technique for minimizing the perceptual impact of embedding watermarks in digital images. As described in the abstract, relative extrema are chosen as signature points in which watermarks are placed. As this relates to the first interpretation of claim 25, the signature is applicant's independent information including a digital watermark. The visual image is applicant's carrier signal. As stated in line 4 of page 4, the signature is encoded "very inconspicuously" or steganographically. The random selection of the extrema, described in lines 39-42 of page 4, reads on a ciphering technique.

Powell et al. also anticipates the second interpretation of "stega-cipher"; selection of the extrema, as mentioned in, for example, lines 33-35 of page 4, anticipates selecting a portion of the carrier signal that will minimally display an inserted watermark. As described in the last line of the paragraph (lines 39-42 of page 4), certain extrema can be chosen from amongst all extrema randomly. The random function is combined with potential signature points, with the result both being used to insert the signature into the carrier and reading on a key. The combined result is specifically referred to in the paragraph bridging pages 4 and 5 as x-y coordinates of the signature point.

The above discussion of Powell et al.'s applicability to the second interpretation of "stega-cipher" largely describes the third interpretation as well. The Difference of Averages technique disclosed in lines 33-35 of page 4 is an algorithm to steganographically determine where in an image (a type of carrier signal) data can be hidden "in plain view". Potential signature points are combined with some form of randomness, which reads on applicant's random or pseudo random seed, to select actual points for signature insertion. The combined randomness and potential signature points is a key, described as x-y coordinates, that is used to randomly map the signature (independent information including a watermark) into the image (carrier signal).

With respect to claim 26, pixilated images anticipate a stream of digital samples, those being the different pixels. Claim 27 is anticipated by Powell et al.'s discussion of distributing analog media in lines 8-10 of page 10. The analog media includes continuous analog waveforms, such as some film clips. In the paragraph starting at line 8 of page 2, Powell et al. describe imbuing images with ownership information, which reads on claim 28.

Using the first interpretation of "stega-cipher", claim 29 is anticipated by the discussion of decoding the digital signature that starts at line 57 of page 4 and runs through line 14 of page 6. By the third definition, the x-y coordinates of the signature are used to audit, or decode, a signed image. As such, a key that is based on potential signature points and a random seed is used to decode independent information from a carrier signal.

Claims 30-32 are rejected for largely the same reasons as claims 26-28. Claim 33 is anticipated by the insertion of the signature into the original image, with the original carrier signal being the original picture and the first derivative signal being the signature-embedded image. In lines 8-11 of page 5, Powell et al. present the situation where the signature-embedded image is altered; the result is more different than the original than the signature-embedded image. The alteration, be it significant color alteration, size reduction, or distinct-pixel-value reduction, can destroy the watermark, but only at the cost of significant degradation of the original image. Thus the limitations of claim 35 are anticipated.

Pixel values in Powell et al. are modified by +/-2-10%. When this change results in a change of one bit, claim 36 is anticipated. Powell et al.'s description of subtracting an original image with a potentially signature-embedded image in lines 51-56 of page 5 anticipates mapping a single sample (pixel) in a range of sample values which indicate a particular message bit value to decode the signature from the signature-embedded image. Thus claim 37 is anticipated. Pixels are spectral values, and thus claim 38 is anticipated. The potential signature points read on applicant's map table and claim 39. Claims 62 and 63 are anticipated because changes caused by the addition of signatures are "very" inconspicuous, as mentioned in line 4 of page 4.

4. Claims 34, 40-43, and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Schneier.

Powell et al. teaches placing digital signatures into images with a key. They do not say that mask sets are used. Chapter 10 of Schneier deals with the Digital Encryption Standard. DES effectively uses a 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's one or more random or pseudo-random series of bits in a mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. As such, the limitations that are unique to clauses c) and d) of claims 40 and 46 are clearly shown by DES as described in Schneier. The elements of claim 41 are shown by the starting vector, message (independent information in the claims), and padding of DES. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. DES is an encryption standard that protects data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the signature of Powell et al. with DES to protect the data. Clause e) in claims 40 and 46 is anticipated by Powell et al. using signature data that is necessarily selected prior to embedding.

5. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Powell et al. and Schneier teach encrypting digital signatures and placing them into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Powell et al. and Schneier's system.

6. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Powell et al. and Schneier teach encrypting digital signatures and placing the resulting cryptograms into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Powell et al. and Schneier. Operating on only the start of message delimiter would protect encrypted data.

7. Claims 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Barton.

Powell et al. teach embedding digital signatures into information. They do not say that the signatures are each unique. In lines 20-33 of column 4, Barton teaches including sequence data with authentication data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Serialized signatures could also deter cryptanalysis attacks.

8. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Barton as applied to claim 54 above.

Powell et al. teach embedding digital signatures as watermarks into information with a key. They do not say that the signature is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as verification. Digital signature with message appendix is a common term for this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information. As it applies to claim 55, the inherent task of calculating the number of sample windows needed to contain a complete signature would be extended to calculating the number of sample windows required to hold a complete signature and its hash. With respect to claim 56, computing a hash that is insensitive to changes introduced by the signature-embedding or watermarking process allows the signature to be recreated without removing the watermark and is hence an obvious feature.

9. Claims 26, 30, and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Barton.

Bender et al. teach encrypting digital watermarks and placing them into information with a key. They do not say that the information includes a stream of digital samples. Barton teaches embedding authentication information within a stream of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate digital sample streams as in Barton with the key-encrypted watermarks of Bender et al.

Bender et al. teach encrypting digital watermarks and placing them into information with a key. They do not say that each sample has unique watermark information. In lines 20-33 of column 4, Barton teaches including sequence data with the authentication data. The authentication data is a reduced representation of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Serialized and hence unique watermarks also deter cryptanalysis attacks.

Pre-processing sample windows is inherent, as is determining which and how many windows will contain watermark information.

10. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al.

Bender et al. teaches encrypting digital watermarks and placing them into information with a key. He does not say that the information is then modified. Encryption modifies data. Official notice is taken that encrypting information in order to protect the data from unauthorized viewing is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it.

11. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Morris.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that one bit is read out of every sample for the watermark. In lines 50-

52 of the third column, Morris says that the human ear cannot detect the difference between a sound value of 64000 and 64001. This would be a one-bit change of the least significant bit. As taught by Morris, these small changes can be used to carry identification codes. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to discretely carry the watermark information of Bender et al. in the least significant bits as taught by Morris.

12. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Powell et al. (5930377).

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that samples are mapped to extract bits of information. As is explained in their abstract and diagrams, Powell et al. teach a method of embedding a digital watermark that requires use of a map of an image to determine the places to embed the watermark. This method is advantageous because, as explained in lines 42-43 of column 1, it is resistant to image modification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the mapping techniques of Powell to the encryption system of Bender et al. so as to make the data's watermark resistant to data modification.

13. Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Braudaway et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not set out that the watermark is used in any specific manner.

By watermarking the data, Braudaway et al.'s method creates a first derivative encoded signal. It is inherent that attempts to decode the watermark without the proper key would further obfuscate the information. It was once theorized that encrypting information with two keys in order to strengthen security could in fact be mimicked by using one key that would possibly be easier to break. Although this theory has since been proven incorrect, the immediate solution was to strengthen security by encrypting with a first key and then decrypting with a non-corresponding second key. Providing information is inherent. In the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark. This change in brightness anticipates claim 38's spectral values. Also in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark. These non-transparent values form a map to meet claim 39. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate any of the teachings of Braudaway into Bender et al.

14. Claims 40-43 and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Schneier.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets containing at least one pseudo random or random series of bits are used. Chapter 10 of Schneier deals with the Digital Encryption Standard. DES effectively uses a 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's one or more random or pseudo-random series of bits in a mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. As such, the limitations that are unique to clauses c) and d) of claims 40 and 46 are clearly shown by DES as described in Schneier. The elements of claim 41 are shown by the starting vector, message (independent information in the claims), and padding of DES. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. DES is an encryption standard that protects data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

15. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Bender et al. and Schneier's system.

16. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Bender et al. and Schneier.

17. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Barton as applied to claim 54 above.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as a verifier. Digital signatures with message appendix are a common implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

(11) Response to Argument

1. Applicant disagrees with the 112 rejection of claims 25-63. As noted by applicant the rejection has arisen from use of the term “stega-cipher”. Applicant contends that support exists for the term and that, if required for applicant's given definition of “stega-cipher”, the specification would provide support. The examiner does not dispute that the term “stega-cipher” was present in the specification at the time of filing. However, the features that applicant considers to be inherent to the term, as evidenced by applicant's legal representation defining “stega-cipher” in terms of those features, are not supported by the specification, and thus applicant is not shown to have been in possession of what applicant apparently believes to be the invention when the patent was filed.

2. As applicant notes, “stega-cipher” was introduced after an interview. The parties agreed that the inclusion of “steganographic key” would overcome the then outstanding rejections of the independent claims. Applicant opted to substitute “stega-cipher” for “steganographic key”, which, as applicant must have presumed, also overcame the outstanding rejections. When updating the search, the examiner came across a reference that anticipates the claims, Bender et al. A new rejection followed. As applicant notes, the examiner put forth no 112 rejections. At this point in the prosecution, none were warranted. Simply put, on its face, “stega-cipher” has a definite meaning. Steganography has been defined above; a cipher is “a method of transforming a text in order to conceal its meaning”. (Based on the state of the art, the examiner interprets “text” more broadly to mean “media” and believes that applicant

would agree with this broadening of the definition of cipher. Even given this alteration, the examiner considers this definition to be more narrow than a person of ordinary skill in the art would understand the term to be.) Put together, the two generally indicate a message that is hidden by transforming text. This limitation was all that was read into the claims.

3. Applicant does not include a discussion of the response to the first rejection of the claims reciting "stega-cipher". The response, dated 25 October 2001 (paper 23), brought to light many issues that applicant considered to be inherent to "stega-cipher" that were not included in the examiner's understanding of the term. On page 4 of response, applicant says that "the stega-cipher being used in the present invention is not . . . limited [to the same key being used for encoding and decoding]." Where does the term "stega-cipher" mandate this limitation? "Bender's 'key' in not ciphered in any manner, but is simply a pseudo-random sequences based on the white noise inherent to the signal." Must a key be ciphered in a stega-cipher? How does being a pseudo-random sequence based on white noise preclude Bender's key from being applicable to hiding messages by transforming text? "[T]he actual mapped locations may be different for each copy encoded of a given carrier signal." When did mapping enter into the picture?

4. Applicant goes on to give a broad outline of what is considered to be part of "stega-cipher" on page 5, saying, "the steganographic portion of the stega-cipher seeks to identify locations within the carrier signal where information may be stored, but it is the cipher portion of the stega-cipher determines which of those identified locations will

be actually used." (The examiner has relied on this passage, among others, to formulate guidelines for the meaning of stega-cipher and the second interpretation of the claims.) Again though, the limitations that applicant apparently considers to be inherent to "stega-cipher", (the incompatibility of pseudo-random keys based on white noise, etc.), are not manifested in its description.

5. Please note also that applicant generally refers to "the stega-cipher being used in the present invention". This nomenclature implies that there are other stega-ciphers that may not include the limitations that applicant views as part of the invention. As such, the examiner's initially broad understanding of "stega-cipher" is appropriate.

6. At some point after sending an advisory action pertaining to the above-discussed response, the examiner came across another reference that anticipates the independent claims, EP-Powell et al., in proceedings unrelated to the present application. Applicant and examiner, subsequently, had a brief telephone conversation, the focus of which the examiner does not remember, in which the examiner mentioned that applicant would be well served to peruse EP-Powell and two other disclosures relevant to watermarking. Applicant and examiner then decided that an interview looked like the most expedient way to resolve the issues of the application.

7. During the interview, applicant gave a definition of stega-cipher. In remarks about the interview, applicant slightly altered the definition and provided general support therefor. However, applicant failed to support one of the limitations of the definition, that being that the independent information ("message data" in the definition) is used to generate the key that maps the independent information into a carrier signal. Applicant

cites several pages of the specification in support of this term, none of which actually shows generating a key based on the definition's message data. The discrepancy between applicant's given definition and the support found in the specification mandated the 112 rejection.

8. In the current response, applicant analyzes the 112 rejection, noting that a key, the primary mask, has a bit length equal to the number of elements in each sample window. This corresponds to the definition's use of potential data location information as an input of the key, but there is no teaching of the generation of a key based on the definition's message data. Applicant goes on to say that "the message data itself is part of the key in that it is placed within the carrier data." By itself, this does not prove that the key is based on the message data, so applicant explains further by saying that "the message and the key are entangled in the embedding process because the key determines where the message bits are located." This directly refutes applicant's idea that the key is based on the message by highlighting that the two are used together after the key has been created. Applicant rolls on, though, noting that the minimum length of the key is the length of the message data. Again, this does not require that the key be based on the message data. In fact, as applicant has cited, the length of the primary mask is equal to the sample window size in samples, which teaches away from the idea that the message data is used to generate the key. Additional citations (specification: page 26, lines 13-18 and pages 54-64) similarly do not teach generating a key that is based on the definition's independent information.

9. In the arguments against the rejections under 35 USC 102 and 103, applicant concludes that the examiner has misread both Bender et al. and EP-Powell. This conclusion seems to largely be based on the first sentence of the 103 rejections, "[Reference] teaches encrypting digital watermarks into information with a key." Applicant does admit that the references teach encoding watermarks into information. Bender et al., as described in the rejection, use a key to encrypt watermarks as part of the run-up to inserting the watermark in the signal. Given the teaching of encryption prior to insertion, the characterization of Bender et al. as "encrypting" watermarks into information with a key is fair. Similarly, EP-Powell uses a key to select alterations to an image as a way to insert an hidden message. In this way, the meaning of the hidden message is concealed. As such, applicant's position that the examiner has misread the references is shown to be groundless. Applicant's error stems largely from a limited conceptualization of encryption, which applicant says "seeks to change the underlying [to be watermarked] data so that it is no longer recognizable." While not incorrect, the preceding fails to recognize that the watermark itself can be encrypted. Despite the applicability of the examiner's original wording, the first sentences of the 103 rejections have been changed to avoid further confusion.

10. Applicant found offensive a previous explanation of the language discussed in the previous paragraph, saying that it "demonstrates that the Examiner is construing Bender and Powell based entirely upon the teachings of the present invention. For example, there is no passage in Powell or Bender that describes embedding a watermark using techniques derived from cryptography <u>and</u> steganography." Contrary

to this assertion, the 102 rejections above clearly show that both EP-Powell and Bender et al. describe embedding a watermark using techniques derived from both cryptography and steganography.

11. The entirety of applicant's arguments specifically against the 102 rejection based on Bender et al. is based on features that are not in the claims. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a stega-cipher not being a pseudo-random sequence modulated at a known rate, ciphering of a key, reliance on only the stega-cipher in decoding, stega-ciphers minimize the bits that are being encoded) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

12. Applicant's traversal of the 102 rejection based on EP-Powell is based on a misreading of the cited section. Applicant repeats the cited section and then dismisses it as saying that EP-Powell teaches "that signature points may be chosen 1) by identifying relative extrema points, or 2) randomly." The cited section actually teaches first identifying a plurality of relative extrema points and then choosing from that plurality a number of signature points. The latter choosing can be done randomly. As such, signature points must be chosen by identifying relative extrema points and are taught, in one embodiment, as being chosen randomly. An accurate reading of the cited passage shows a person of ordinary skill in the art that the claims are clearly anticipated.

Nevertheless, a detailed description of how EP-Powell anticipates several interpretations of the claims has been given in the rejection.

13. Applicant cites four portions of a stega-cipher that EP-Powell allegedly fails to disclose: no cipher, no key to encode or decode, no insertion of independent data into a carrier signal, and no relationship between the message, signal and key. Based on the definition of cipher given above (page 21), the signature in EP-Powell is broken up, thereby being altered, and concealed by being imperceptibly embedded into an image. The combination of the randomness and the potential signature points constitutes a key that is used to encode. The signature is clearly inserted into the image, where the signature reads on independent information and the image is a carrier signal. Finally, the relationship, as disclosed by EP-Powell, between the message (signature), signal (image), and key is that the key is used to choose points within the image at which to insert the signature.

14. Applicant continues the rebuttal by citing the key generated from message data, a feature for which applicant has, as of yet, failed to show support in the specification. The alleged limitation has been rejected under 35 USC 112. Contrary to applicant's assertion, using a source of randomness to select extrema is the same as using a cipher to do so, as shown in the rejections above.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the impermissible use of an original carrier signal to decode the independent information) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant posits that the signature of EP-Powell is not independent information. The signature is a distinctly separate set of bits than the image and as such clearly independent. Nevertheless, applicant's reasoning deserves a more thorough examination. Applicant notes that an original pixel value is changed to a new value that is dependent on the original value. However, this new value is not the signature. Rather, the difference (positive or negative) between the old and new pixel values represents a bit of the independent information. In contrast to applicant's assertion that the signature is dependent on the initial pixel value, the representation of the signature in the image uses a difference between the new value and the initial pixel value. An apparent extension of applicant's argument is that any change to the carrier signal would make the embedded signal dependent upon the carrier. Of course, applicant's invention embeds data in a carrier signal, and thus this argument seems to be irrelevant to not only Powell et al., but also the instant invention.

15. Applicant's final argument with respect to the 102 rejections using EP-Powell is that the reference does not show a key being used in the decoding of the watermark. In the paragraph spanning pages 4 and 5, EP-Powell specifically teaches auditing a signed image with a signature that is "stored by associating the bit value of each signature point together with x-y coordinates of the signature point." The x-y coordinates read on a key. Auditing reads on decoding.

16. Applicant gives a blanket argument to all 103 rejections, saying that there is no motivation to combine the references, specifically citing Barton and Schneier as lacking a reason to combine. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, added security would motivate one to incorporate the teachings of Schneier into EP-Powell and Bender et al. Barton's teachings provide assurances that data is correctly ordered and all present (lines 30-33 of column 4), which is beneficial and hence a motivation to employ the teachings of Barton in EP-Powell and Bender et al.

17. As shown above, both EP-Powell and Bender et al. anticipate various interpretations of "stega-cipher".

18. Applicant mischaracterizes the combination of EP-Powell and Schneier, saying that Schneier would teach encrypting EP-Powell's image. While this combination could be implemented, a more logical joining is the encryption of the signature prior to embedding; in this method, the focus of EP-Powell (a minimally changed image) would be maintained despite the incorporation of Schneier. Motivation to combine the two, given in the rejection and in the paragraph two above this one, is the upgrade in security provided by encrypting the hidden image, thereby protecting it in a second way.

19. Applicant opines that the combination of Schneier and EP-Powell fails to disclose the claimed invention. The only claim limitation that applicant cites as being absent from the combination of references is "mask set". A mask set is a series of random or pseudo-random bits. The key in DES is a series of random or pseudo-random bits. As such, applicant's statement that "there is no 'mask set' in a DES cipher" is clearly wrong.

20. With respect to claim 34 as rejected by Bender et al., the encryption of the watermarked data (first derivative encoded signal) produces encrypted watermarked data (second derivative encoded signal).

21. Applicant's comments with respect to the combination of Bender et al. and Schneier are flawed in the same manner as applicant's analysis of the combination of Schneier and EP-Powell.

22. With respect to applicant's commentary on the impropriety of combining EP-Powell with Barton, applicant begins with the spurious observation that EP-Powell "teaches replacing a pixel value with a new value that is dependent upon the initial value . . .." Applicant had previously argued that this dependence made the data represented by the difference between the initial and new pixel values dependent upon the initial pixel value. How this is germane to Barton is unclear. Applicant confuses the two references, saying that it is Barton "where the pixel values are adjusted only a positive or negative amount" and EP-Powell that contains sequence data. In fact, data that is embedded in EP-Powell is represented as bits by slightly altering some pixel values. The sequence data and signature of Barton would be embedded in the same

fashion. Applicant's description of EP-Powell's signature as "a visual pattern" is overly simplistic. EP-Powell's signature is a series of bits that are embedded into an image. Applicant argues that EP-Powell's signatures are different than Barton's but never shows how, merely noting that EP-Powell does not use "existing digital signatures". Nowhere does applicant make the case that Barton is limited to EP-Powell's "existing digital signatures". As such, the general signatures taught by Barton are applicable to EP-Powell.

23. Applicant posits that neither Barton nor EP-Powell teach multiple watermarks in a sample stream. Barton clearly teaches different and hence multiple watermarks in lines 30-33 of column 4 by teaching sequence numbers added to frames. Applicant's discussion of the possible benefits of multiple watermarks is unrelated to the claim language and hence irrelevant to the patentability of the claims. Applicant discusses the applicability of Barton to the claims saying that the feature of "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream" is not present. By way of explanation, applicant notes that the sequence numbers added to the watermarks are unique to the underlying data, and hence implicitly not the watermarks. Of course, the watermarks have a one-to-one relationship to the underlying data, and hence adding sequence data that is unique to the underlying data to the watermarks gives the watermarks unique data.

24. Applicant's commentary on the combination of Barton and Bender et al. is unpersuasive for the same reasons as were the arguments against the combination of Barton and EP-Powell.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
DJM
September 22, 2003

Conferees
Gilberto Barrón
Matthew Smithers

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Wiley Rein & Fielding
1776 K Street, N.W.
WASHINGTON, DC 20006

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134